基于 STBC 的无线认知 NOMA 系统物理层安全性能研究

李美玲[1],田莉莉[1],杨晓霞[1],李 莹[1],王安红[1],
董增寿[1],Sami Muhaidat[2],Mehrdad Dianati[3]
(1. 太原科技大学电子信息工程学院,山西太原 030024;2. Khalifa 大学,阿联酋阿布扎比;3. 华威大学,英国英格兰)

摘 要: 基于非正交多址接入(NOMA,Non-Orthogonal Multiple Access)的认知无线电(CR,Cognitive Radio)网络物理层传输面临主用户干扰和第三方窃听双重干扰威胁.本文提出利用空时编码(STBC,Space Time Block Coding)技术提高认知用户物理层安全性能,推导了任意认知用户的安全中断概率闭合表达式.通过蒙特卡洛仿真进行验证,结果表明,所提 STBC-CR-NOMA 相比未采用 STBC 编码方案的 CR-NOMA 可以明显提高用户的安全中断概率,且随着认知发射功率的增大,近端用户安全中断性能提高越大,而远端用户安全中断性能提升受认知基站发射功率的影响较小.仿真结果还表明,通过调整功率分配系数对远端用户和近端用户的安全中断性能影响不同.

关键词: 非正交多址接入;认知无线电;空时编码;窃听者;物理层安全;安全中断概率
中图分类号: TN911.1 **文献标识码:** A **文章编号:** 0372-2112 (2020)03-0463-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.03.007

On the Secrecy Performance of NOMA-Based Cognitive Radio Networks with STBC

LI Mei-ling[1],TIAN Li-li[1],YANG Xiao-xia[1],LI Ying[1],WANG An-hong[1],
DONG Zeng-shou[1],Sami Muhaidat[2],Mehrdad Dianati[3]
(1. *School of Electronic and Information Engineering,Taiyuan University of Science and Technology,Taiyuan,Shanxi* 030024,*China*;
2. *University of Khalifa,Abu Dhabi,The United Arab Emirates*;3. *University of Warwick,England,UK*)

Abstract: The physical layer transmission faces the interference from primary users and eavesdroppers in cognitive radio networks based on non-orthogonal multiple access (CR-NOMA). In this paper,Alamouti space-time block coded (STBC) is utilized to improve the physical layer security transmission performance. The closed-form expressions for the security outage probability of all secondary users are derived. We provide extensive Monte-Carlo simulation results to corroborate the analysis. The results show that the security outage probability of stronger cognitive users is improved by the proposed STBC-NOMA-based CR compared with the traditional NOMA-based CR. Moreover,the security outage probability of the stronger cognitive users experiences performance enhancement with the increase of the cognitive transmission power,whilst the security outage probability of weaker cognitive users will be less impacted by the transmission power. In addition,we demonstrate that the power allocation coefficients will have different impact on the stronger cognitive users and the weaker users.

Key words: non-orthogonal multiple access;cognitive radio;space time block code;eavesdropper;physical layer security;security outage probability

收稿日期:2019-05-22;修回日期:2019-09-08;责任编辑:覃怀银
基金项目:国家自然科学基金(No.61672373);山西省高等学校科技创新项目(No.201802090);山西省互联网 +3D 打印协同创新中心项目;山西省科技创新团队项目(No.201705D131025);山西省 1331 工程重点创新团队项目;山西省重点研发计划项目(No.201903D121117);山西省研究生优秀创新项目(No.2019SY491)

1 引言

非正交多址接入(NOMA,Non-Orthogonal Multiple Access)技术通过利用功率域在相同的资源块上(时域、频域或码域)为多个用户服务,可以有效提高频谱效率,是5G移动通信系统的关键技术之一,已经得到了学术界的广泛关注[1].在功率域NOMA系统中,接收机利用连续干扰删除(SIC,Successive Interference Cancellation)技术来避免同道干扰从而获取期望信号.文献[2]提出了一种通用的功率域NOMA,分别对理想SIC和非理想SIC下的NOMA用户中断性能进行了分析.文献[3]对基于双跳中继协作的NOMA性能进行了研究,研究表明通过用户间的协作可进一步提高NOMA传输性能.为了在传统多用户单天线协作传输的基础上,进一步提高频谱利用率,在文献[4]中,作者提出了一种两阶段的协作中继方案,在协作时采用Alamouti空时编码(STBC,Space Time Block Code)方案以提高传输效率及可靠性.文献[5]将分布式STBC方案应用于下行链路NOMA传输系统中,结果表明所提方法可有效提升小区边缘用户性能.

认知无线电技术(CR,Cognitive Radio)作为一种可有效提高频谱利用率的手段与NOMA方案相结合,可进一步满足未来大规模接入和超低时延传输的实际通信环境[6].文献[7]将NOMA技术应用于下行无线认知网络,认知用户(CUs,Cognitive Users)作为中继转发主用户(PUs,Primary Users)信号.由于认知无线网络的动态和广播特性,使得认知无线网络(CRN,Cognitive Radio Networks)比传统网络更易受到窃听攻击.物理层安全(PLS,Physical Layer Security)技术从信息论的角度出发,解决无线网络安全问题,成为近年来研究热点.最近Feng等人基于underlay模式对用户安全中断概率进行了分析[8].Zhou等人提出利用同步无线信息功率转换技术最大化CR能量有效性,基于人工噪声的协作方案,提高CR-NOMA主网络的安全性[9].

本文考虑基于underlay的认知功率域NOMA下行传输链路且在无线传输过程中存在第三方窃听者的实际场景.在认知传输阶段,配置多天线的认知基站利用STBC方式发送下行NOMA信号,从而提高CR-NOMA系统安全性能,通过安全中断概率衡量所提基于STBC的CR-NOMA(STBC-CR-NOMA)物理层安全传输性能.推导了STBC-CR-NOMA次网络中任意远端用户和近端用户的安全中断性能闭合表达式,并通过蒙特卡洛仿真进行了验证.结果表明通过采用STBC方案可大幅度降低近端用户的安全中断概率,且增加认知基站的发射功率或增大主窃听链路比(MER,Main-to-Eavesdropper Ratio)均可提高任意认知用户的物理层安全性能,而调整发射功率比不一定能改善认知用户的物理层安全性能.

2 系统模型

如图1所示基于underlay的STBC-CR-NOMA系统模型中,主网络由主发射机(PT,Primary Transmitter)和主接收机(PR,Primary Receiver)构成,认知网络由配备有两根发射天线(S_1,S_2)的认知基站(CBS,Cognitive Base Station)和具有单接收天线的认知用户构成.认知网络以机会式接入授权频谱进行认知传输,即只有当认知用户检测到空闲频谱资源时,认知网络才会利用空闲频谱资源进行通信,不会故意干扰主用户通信.同时在信号传输过程中,窃听者(E,Eavesdropper)会试图截获认知传输信号.用$\hat{H}=H_0$、$\hat{H}=H_1$分别表示授权频谱未被占用和被占用时的情况.当主用户返回通信而认知用户无法及时释放授权频谱资源时,考虑主网络对认知网络的干扰功率为ρ_P,用P_d和P_f分别代表检测授权频谱是否被占用时检测正确的概率和检测错误的概率$P_d=\Pr(\hat{H}=H_1|H_1)$,$P_f=\Pr(\hat{H}=H_1|H_0)$.

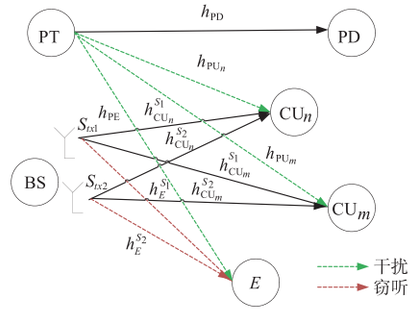


图1 STBC-CR-NOMA系统

本文考虑CBS配置两个发射天线,基于NOMA通过STBC与已成功配对的任意两个认知用户(远端认知用户CU_m和近端认知用户CU_n)同时通信.CU_j,$j\in\{n,m\}$在时隙T_1和T_2接收来自天线S_1和S_2的信号,如表1所示.其中,$\theta_i=\sqrt{a_n\rho_S}x_{n_i}+\sqrt{a_m\rho_S}x_{m_i}$为天线$i$发送的NOMA信号,$a_n$和$a_m$是功率分配系数,$a_n+a_m=1$,$a_m>a_n$.$h_{PU_j}$、$h_{CU_j}^{S_i}$、分别为PT→$CU_j$和$S_i$→$CU_j$链路的信道衰落系数.$x_P$为PT的传输信号,$n_{CU_j}^{S_i}\sim CN(0,1)$,$i\in\{1,2\}$为天线$S_i$→$CU_j$链路上的加性高斯白噪声(AWGN,Additive White Gaussian Noise).

在BS向CU_n、CU_m广播信号的同时,窃听者E也会收到由BS发出的复合信号,则E在时隙T_1和T_2接收到的来自天线S_1和S_2的信号,如表2所示.其中,$h_E^{S_i}$,$i\in\{1,2\}$,h_{PE}分别代表S_i→E和PT→E链路的信道衰落系数,$n_E^{S_i}\sim CN(0,\sigma_e^2)$,$i\in\{1,2\}$为$S_i\to E$链路上的AWGN.

表 1　CU_j接收到的信号

	S_1	S_2
T_1	$y_{CU_j}^{S_1-T_1}=h_{CU_j}^{S_1}\theta_1+h_{PU_j}\sqrt{\rho_P}x_P+n_{CU_j}^{S_1}$ (1)	$y_{CU_j}^{S_2-T_1}=h_{CU_j}^{S_2}\theta_2+h_{PU_j}\sqrt{\rho_P}x_P+n_{CU_j}^{S_2}$ (2)
T_2	$y_{CU_j}^{S_1-T_2}=-h_{CU_j}^{S_1}\theta_2^*+h_{PU_j}\sqrt{\rho_P}x_P+n_{CU_j}^{S_1}$ (3)	$y_{CU_j}^{S_2-T_2}=h_{CU_j}^{S_2}\theta_1^*+h_{PU_j}\sqrt{\rho_P}x_P+n_{CU_j}^{S_2}$ (4)

表 2　E 接收到的信号

	S_1	S_2
T_1	$y_E^{S_1-T_1}=h_E^{S_1}\theta_1+h_{PE}\sqrt{\rho_P}x_P+n_E^{S_1}$ (5)	$y_E^{S_2-T_1}=h_E^{S_2}\theta_2+h_{PE}\sqrt{\rho_P}x_P+n_E^{S_2}$ (6)
T_2	$y_E^{S_1-T_2}=-h_E^{S_1}\theta_2^*+h_{PE}\sqrt{\rho_P}x_P+n_E^{S_1}$ (7)	$y_E^{S_2-T_2}=h_E^{S_2}\theta_2^*+h_{PE}\sqrt{\rho_P}x_P+n_E^{S_2}$ (8)

根据物理层安全传输理论[10],我们将安全容量定义为主信道信道容量与窃听信道容量之差,因此,CU_i的瞬时安全容量可描述为:

$$C_{S,CU_j}=\max\{[C_{CU_j}-C_{E\to CU_j}],0\} \tag{9}$$

本文考虑 CBS 采用 STBC 发送 NOMA 信号,因此,用户将对不同时刻接收到的不同天线信号进行合并然后利用 SIC 技术从而获得更高的传输速率. 作为近端用户的 CU_n首先通过 SIC 技术提取 CU_m信号 x_{m_1}和 x_{m_2},然后再解自身信号 x_{n_1}和 x_{n_2},因此根据式(1)~(4)可得 BS→CU_n链路的信道容量为:

$$C_{CU_n}=\frac{1}{2}\log_2(1+\min(\gamma_{n,1}^{\alpha},\gamma_{n,2}^{\alpha})) \tag{10}$$

其中:$\alpha=\begin{cases}0,\hat{H}=H_0\\1,\hat{H}=H_1\end{cases}$,

$$\gamma_{n,1}^{\alpha}=\frac{a_m\rho_S\sum_{i=1}^{2}|h_{CU_n}^{S_i}|^2}{a_n\rho_S\sum_{i=1}^{2}|h_{CU_n}^{S_i}|^2+\alpha\rho_P|h_{PU_n}|^2+1},$$

$$\gamma_{n,2}^{\alpha}=\frac{a_n\rho_S\sum_{i=1}^{2}|h_{CU_n}^{S_i}|^2}{\alpha\rho_P|h_{PU_n}|^2+1},$$

$\alpha=0$ 表示授权频谱未被占用时的情况,$\alpha=1$ 表示授权频谱被占用的情况.

同理,我们考虑窃听者具有较强的截获能力,与授权用户一样可利用 SIC 对每个用户信号进行解码,根据式(5)~(8)可得 E 窃听 CU_n信号时可获得的信道容量为:

$$C_{E\to CU_n}=\frac{1}{2}\log_2\left(1+\underbrace{\frac{a_n\rho_S\sum_{i=1}^{2}|h_E^{S_i}|^2}{a_m\rho_S\sum_{i=1}^{2}|h_E^{S_i}|^2+\alpha\rho_P|h_{PE}|^2+1}}_{\gamma_{E,n}^{\alpha}}\right) \tag{11}$$

根据功率域 NOMA 原理,作为远端用户的 CU_m在解码自身信号 x_{m_1}和 x_{m_2}时,将 CU_n信号作为干扰,因此,根据式(1)~(4)可得 CU_m可获得的信道容量为:

$$C_{CU_m}=\frac{1}{2}\log_2\left(1+\frac{a_m\rho_S\sum_{i=1}^{2}|h_{CU_m}^{S_i}|^2}{a_n\rho_S\sum_{i=1}^{2}|h_{CU_m}^{S_i}|^2+\alpha\rho_P|h_{PU_m}|^2+1}\right) \tag{12}$$

同理,根据式(5)~(8)可得 E 窃听 CU_m信号时可获得的信道容量为:

$$C_{E\to CU_m}=\frac{1}{2}\log_2\left(1+\frac{a_m\rho_S\sum_{i=1}^{2}|h_E^{S_i}|^2}{a_n\rho_S\sum_{i=1}^{2}|h_E^{S_i}|^2+\alpha\rho_P|h_{PE}|^2+1}\right) \tag{13}$$

3　安全中断性能

本文考虑基于 underlay 的认知网络,只有当认知用户检测到频谱空闲时,才能利用检测到的频谱资源实现认知传输. 而认知用户可能正确检测到空闲频谱$\{H_0|\hat{H}=H_0\}$也可能错误地检测到空闲频谱$\{H_1|\hat{H}=H_0\}$(即实际主用户占用频谱情况),此时,主用户的传输就会对认知传输产生干扰. 我们定义认知基站传输认知用户信号时,若在认知用户接收信号的过程中可获得的信道容量小于窃听链路截获该信号可获得的信道容量时,认知用户传输发生安全中断. 综上所述,根据全概率公式,安全中断概率为检测到授权频谱未被占用且检测结果正确的条件下认知用户发生安全中断的概率和检测到授权频谱未被占用但检测结果错误的条件下认知用户发生安全中断的概率之和. 对于任意用户CU_j,当其检测到 PU 空闲从而执行认知传输时的安全中断概率为:

$$\begin{aligned}P_{SOP}^{CU_j}&=\Pr(C_{CU_j}\leqslant C_{E\to CU_j}|\hat{H}=H_0)\\&=\pi_0\Pr(C_{CU_j}\leqslant C_{E\to CU_j}|H_0,\hat{H}=H_0)\\&\quad+\pi_1\Pr(C_{CU_j}\leqslant C_{E\to CU_j}|H_1,\hat{H}=H_0)\end{aligned} \tag{14}$$

其中:$\pi_0=\frac{P_0\bar{P}_f}{P_0\bar{P}_f+(1-P_0)\bar{P}_d}$,$\pi_1=\frac{(1-P_0)\bar{P}_d}{P_0\bar{P}_f+(1-P_0)\bar{P}_d}$,

$\bar{P}_f = 1 - P_f, \bar{P}_d = 1 - P_d$.

由于近端用户 CU_n 和远端用户 CU_m 可获得的信道容量不通,下面我们分别讨论 CU_n 和 CU_m 的安全中断概率.

3.1 CU_n 的安全中断概率

根据式(14),令 $P^1_{CU_n} = \Pr(C_{CU_n} \leqslant C_{E\to CU_n} | H_0, \hat{H} = H_0)$, $P^2_{CU_n} = \Pr(C_{CU_n} \leqslant C_{E\to CU_n} | H_1, \hat{H} = H_0)$,则当 CU_n 检测到 PU 空闲从而执行认知传输时,CU_n 的安全中断概率为:

$$P^{CU_n}_{SOP} = \pi_0 P^1_{CU_n} + \pi_1 P^2_{CU_n} \tag{15}$$

根据式(10)和式(11),可以得到

$$P^1_{CU_n} = \Pr(\min(\gamma^0_{n,1}, \gamma^0_{n,2}) \leqslant \gamma^0_{E,n}) = \underbrace{\Pr(\gamma^0_{n,1} \leqslant \gamma^0_{E,n}, \gamma^0_{n,1} \leqslant \gamma^0_{n,2})}_{P^{1-1}_{CU_n}} + \underbrace{\Pr(\gamma^0_{n,2} \leqslant \gamma^0_{E,n}, \gamma^0_{n,1} > \gamma^0_{n,2})}_{P^{1-2}_{CU_n}} \tag{16}$$

$$P^2_{CU_n} = \Pr(\min(\gamma^1_{n,1}, \gamma^1_{n,2}) \leqslant \gamma^1_{E,n}) = \underbrace{\Pr(\gamma^1_{n,1} \leqslant \gamma^1_{E,n}, \gamma^1_{n,1} \leqslant \gamma^1_{n,2})}_{P^{2-1}_{CU_n}} + \underbrace{\Pr(\gamma^1_{n,2} \leqslant \gamma^1_{E,n}, \gamma^1_{n,1} > \gamma^1_{n,2})}_{P^{2-2}_{CU_n}} \tag{17}$$

本文考虑根据服务质量区分用户,而非根据信道质量区分用户[11]. 在不考虑信道排序情况下,用 W 表示 L 个独立同分布的方差为 λ_0 的指数分布变量,则 W 的分布函数可表示为:

$$F_W(w) = 1 - \exp\left(-\frac{w}{\lambda_0}\right) \sum_{i=0}^{L-1} \left(\frac{w}{\lambda_0}\right)^i \frac{1}{i!} \tag{18}$$

令 $U_1 = \sum_{i=1}^{2} |h^{S_i}_{CU_n}|^2$、$V_1 = \sum_{i=1}^{2} |h^{S_i}_E|^2$、$X_1 = \frac{a_m U_1}{a_n \rho_S U_1 + 1}$、$Y_1 = \frac{a_n V_1}{a_m \rho_S V_1 + 1}$、$Y_2 = \frac{V_1}{a_m \rho_S V_1 + 1}$. 用 $F_Q(x)$ 和 $f_Q(x)$ 表示变量 Q 的分布函数和概率密度函数,根据式(16)并利用式(18)经过分析,当 $y_1 < \frac{a_n}{a_m \rho_S}$ 时,可以得到:

$$P^{1-1}_{CU_n} = \Pr\left(X_1 \leqslant Y_1, U_1 \geqslant \frac{a_m - a_n}{a_n^2 \rho_S}\right) = \int_{\frac{a_m - a_n}{a_n \rho_S}}^{\frac{a_n}{a_m \rho_S}} F_{X_1}(y_1) \frac{a_n y_1}{\lambda_E^2 \varepsilon_y^3} \exp\left(-\frac{y_1}{\lambda_E \varepsilon_y}\right) \mathrm{d}y_1 \tag{19}$$

由于式(19)很难得到精确的结果,我们可以根据 Gaussian-Chebyshe Quadrature 定理[11],令 $G_1(z) = f_{Y_1}(z) \cdot F_{X_1}(z)$, $\tau_n = \cos\left(\frac{2n-1}{2N}\pi\right)$ 且 $z_1 = \frac{a_n a_m - a_{mn}}{2 a_n a_m \rho_S} \tau_n + \frac{a_n^2 + a_m^2 - a_n a_m}{2 a_n a_m \rho_S}$, $a_{mn} = a_m - a_n$, $\vartheta_n = \frac{\pi}{N \rho_S} \sqrt{1 - \tau_n^2}$, 可得 $P^{1-1}_{CU_n}$ 表达式为:

$$P^{1-1}_{CU_n} = \frac{a_n a_m - a_{mn}}{2 a_n a_m} \sum_{n=1}^{N} \vartheta_n G_1(z_1) \tag{20}$$

同理,我们可以先求得 Y_2 的概率密度函数 $f_{Y_2}(x)$ 和 U_1 的分布函数 $F_{U_1}(x)$,令 $G_2(z_2) = f_{Y_2}(z_2) F_{U_1}(z_2)$, $z_2 = \frac{z_1}{a_n}$,利用 Gaussian-Chebyshe Quadrature 定理得到 $P^{1-2}_{CU_n}$ 表达式为:

$$P^{1-2}_{CU_n} = \begin{cases} \frac{a_{mn}}{2a_n^2} \sum_{n=1}^{N} \vartheta_n G_2(z_2) + G_3, & D_1 \\ \frac{\pi}{2N a_m \rho_S} \sum_{n=1}^{N} \sqrt{1 - \tau_n^2} G_2\left(\frac{(\tau_n + 1)}{2 a_m \rho_S}\right), & D_2 \end{cases} \tag{21}$$

其中,D_1:$0.5 < a_m \leqslant 0.618$, D_2:$0.618 < a_m < 1$,

$$G_3 = G_{31}\left(1 - \left(1 + \frac{a_{mn}}{\lambda_{CU_n} a_n^2 \rho_S}\right) \exp\left(-\frac{a_{mn}}{\lambda_{CU_n} a_n^2 \rho_S}\right)\right),$$

$$G_{31} = \left(1 + \frac{a_{mn}}{\lambda_E \rho_S (a_n a_m - a_{mn})}\right) \exp\left(-\frac{a_{mn}}{\lambda_E \rho_S (a_n a_m - a_{mn})}\right).$$

对于式(17),我们可以利用得到式(16)的方法,令 $\varepsilon_{x_2} = a_m - a_n \rho_S x_2$, $\varepsilon_{x_3} = \lambda_{CU_n} + \lambda_{PU_n} \rho_P x_3$, $x = \lambda_{PU_n} \rho_P$, $\varepsilon_{y_4} = \lambda_E + (\rho_P \lambda_{PE} - a_m \rho_S \lambda_E) y_4$, $x_1 = \rho_P \lambda_{PE}$, $x_2 = \rho_S \lambda_E$, $G_5(z_3) = f_{Y_4}(z_3) F_{X_3}(z_3)$, $z_3 = \frac{a_{mn}}{2 a_n^2 \rho_S}(\tau_n + 1)$. 得到如下结果:

$$P^{2-1}_{CU_n} = \frac{a_n a_m - a_{mn}}{2 a_n a_m} \sum_{n=1}^{N} \vartheta_n f_{Y_3}(z_1) F_{X_2}(z_1) \tag{22}$$

$$P^{2-2}_{CU_n} = \begin{cases} \frac{a_{mn}}{2a_n^2} \sum_{n=1}^{N} \vartheta_n G_5(z_3) + G_6, & D_1 \\ \frac{\pi}{2N a_m \rho_S} \sum_{n=1}^{N} \sqrt{1 - \tau_n^2} G_5\left(\frac{(\tau_n + 1)}{2 a_m \rho_S}\right), & D_2 \end{cases} \tag{23}$$

其中, $X_2 = \frac{a_m U_1}{a_n \rho_S U_1 + \rho_P U_2 + 1}$, $X_3 = \frac{U_1}{\rho_P U_2 + 1}$, $Y_3 = \frac{a_n V_1}{a_m \rho_S V_1 + \rho_P V_2 + 1}$, $Y_4 = \frac{V_1}{a_m \rho_S V_1 + \rho_P V_2 + 1}$, $U_2 = |h_{PU_n}|^2$, $V_2 = |h_{PE}|^2$,它们的概率密度函数和分布函数可以根据式(18)得到, $G_{61} = \frac{a_{mn} x \lambda_{CU_n} a_n^2 \rho_S}{(a_n^2 \rho_S \lambda_{CU_n} + x a_{mn})^2} + \frac{a_{mn} + a_n^2 \rho_S \lambda_{CU_n}}{\lambda_{CU_n} a_n^2 \rho_S + a_{mn} x}$,

$$G_{62} = \frac{x_1 x_2 a_{mn}(a_{mn} + a_n a_m)}{(\lambda_E a_n^2 \rho_S + x_1 a_{mn} - a_{m2} a_{mn} x)^2} + \frac{a_{mn} + a_n^2 x_2 - a_m a_{mn} x_2}{a_n^2 x_2 + a_{mn} x_1 - a_m a_{mn} x_2},$$

$$G_6 = G_{61} G_{62} \exp\left(-\frac{a_{mn}}{x_2(a_n a_m - a_{mn})}\right)\left(1 - \exp\left(-\frac{a_{mn}}{\lambda_{CU_n} a_n^2 \rho_S}\right)\right).$$

综合式(15)~(17)和式(20)~(23)即可得到 CU_n 的安全中断概率.

3.2 CU_m 的安全中断概率

基于式(14),令 $P^1_{CU_m} = \Pr(C_{CU_m} \leqslant C_{E\to CU_m} | H_0, \hat{H} = H_0)$, $P^2_{CU_m} = \Pr(C_{CU_m} \leqslant C_{E\to CU_m} | H_1, \hat{H} = H_0)$,则当 CU_m 检测到 PU 空闲从而执行认知传输时,CU_m 的安全中断概率为:

$$P^{CU_m}_{SOP} = \pi_0 P^1_{CU_m} + \pi_1 P^2_{CU_m} \tag{24}$$

根据式(12)和式(13),可得

$$P^1_{CU_m} = \Pr\left(\frac{\sum_{i=1}^{2} |h^{S_i}_{CU_m}|^2}{a_m \rho_S \sum_{i=1}^{2} |h^{S_i}_{CU_m}|^2 + 1} \leqslant \frac{\sum_{i=1}^{2} |h^{S_i}_E|^2}{a_m \rho_S \sum_{i=1}^{2} |h^{S_i}_E|^2 + 1}\right) \tag{25}$$

$$P_{\mathrm{CU}_m}^2=\Pr\left(\frac{\sum_{i=1}^{2}|h_{\mathrm{CU}_m}^{S_i}|^2}{a_n\rho_S\sum_{i=1}^{2}|h_{\mathrm{CU}_m}^{S_i}|^2+\rho_P|h_{\mathrm{PU}_m}|^2+1}\leqslant\frac{\sum_{i=1}^{2}|h_E^{S_i}|^2}{a_n\rho_S\sum_{i=1}^{2}|h_E^{S_i}|^2+\rho_P|h_{\mathrm{PE}}|^2+1}\right)\tag{26}$$

利用得到 CU_n 的安全中断概率计算方法,结合式(26)可以得到 CU_m 的安全中断概率为:

$$P_{\mathrm{SOP}}^{\mathrm{CU}_m}=\frac{\pi_0}{2a_n}\sum_{n=1}^{N}\vartheta_nG_7\left(\frac{\tau_n+1}{2a_n\rho_S}\right)+\frac{\pi_1}{2a_n}\sum_{n=1}^{N}\vartheta_nG_8\left(\frac{\tau_n+1}{2a_n\rho_S}\right)\tag{27}$$

其中,$G_7(y_5)=f_{Y_5}(y_5)F_{X_4}(y_5)$,$G_8(y_6)=f_{Y_6}(y_6)F_{X_5}(y_6)$,$X_4=\dfrac{U_1}{a_n\rho_SU_1+1}$,$X_5=\dfrac{U_1}{a_n\rho_SU_1+\rho_PU_2+1}$,$Y_5=\dfrac{V_1}{a_n\rho_SV_1+1}$,$Y_6=\dfrac{V_1}{a_n\rho_SV_1+\rho_PV_2+1}$.

3.3　复杂度分析

采用 STBC 编码方案可以实现多天线传输,通过增加编码复杂度来提高分集增益. 虽然在发射端设计正交码字会带来一定编码复杂度,但是随着硬件技术的不断发展与成熟,这种编码复杂度及所需要的时间相比传输时间可完全忽略. 此外,在 NOMA 系统中,接收端需要利用 SIC 技术消除干扰. 对于所提出的方案共需执行 4 次 SIC 操作,而在非 STBC 的 CR-NOMA 方案中,共需执行 2 次 SIC 操作. 尽管所提方案需要牺牲一定操作复杂度,但是对于未来通信系统而言,这种操作复杂度是完全可以克服的.

4　仿真结果

本节通过 Monte Carlo 仿真对基于 underlay 的下行认知 NOMA 传输系统存在窃听者时的用户性能进行了验证,并与传统未采用 STBC 方案的下行 CR-NOMA 系统中用户的安全中断概率进行了比较. 如非特别说明,设定 $\lambda_{\mathrm{PU}_n}=\lambda_{\mathrm{PU}_m}=5\mathrm{dB}$、$\lambda_{pe}=\lambda_e=0\mathrm{dB}$、$P_0=0.8$、$P_d=0.99$、$P_f=0.01$、$\rho_P=10\mathrm{dB}$.

图 2 表示 a_m 分别取 0.6 和 0.9 时认知用户 CU_n 和 CU_m 的安全中断概率随认知基站发射功率的变化情况. 其中参数设置为 $\lambda_{\mathrm{CU}_n}=6\mathrm{dB}$、$\lambda_{\mathrm{CU}_m}=3\mathrm{dB}$. 从图 2 中可以看出,$\mathrm{CU}_n$ 的安全中断概率随基站发射功率的增大而减小,这是由于对于 CU_n 来说,增大基站的发射功率在某种情况下减小了 E 窃听 CU_n 信号时信道的信道容量,但对 BS→CU_n 链路的信道容量没有影响,从式(20)可以看出相应关系. 但对于 CU_m 来说增加基站的发射功率,在增强 BS→CU_m 接收信号强度的同时,窃听者 E 截获 CU_m 信号的能力也增强,因此,CU_m 安全中断随基站发射功率的变化较小. 从图中还可以看出与传统未采用 STBC 方案的 CR-NOMA 相比,采用 STBC 可以降低用户安全中断概率,具体地,当基站发射功率为 10dB 时,采用 STBC 方案可以使 CU_n 的安全中断概率降低 10^{-1} 数量级,且随着基站发射功率的增大,安全中断性能提高越明显;对于远端用户 CU_m 而言,不论基站发射功率为多大都可使其安全中断性能改善 8% 左右. 通过对比图 2(*a*)和图 2(*b*)可以看出,提高功率分配系数 a_m,可以大幅度降低近端用户 CU_n 的安全中断概率,但是远端用户 CU_m 的安全中断概率改善却不明显.

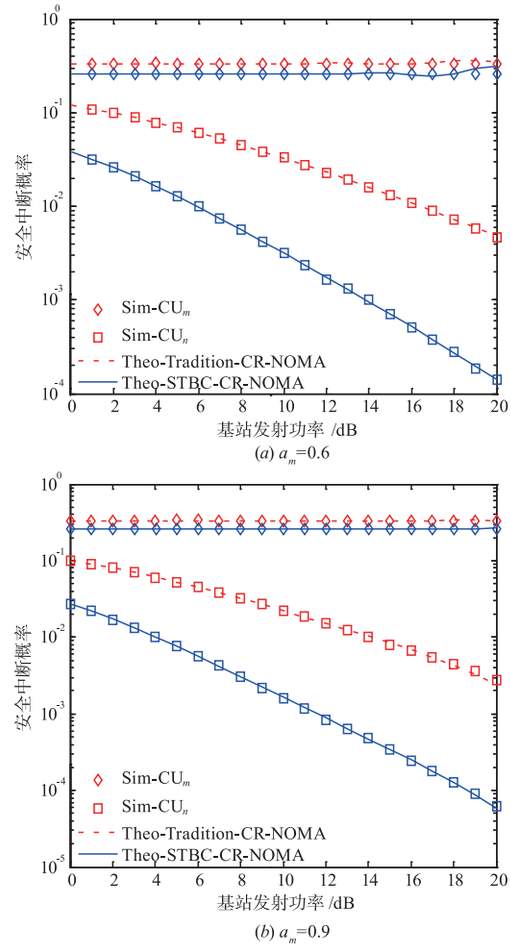
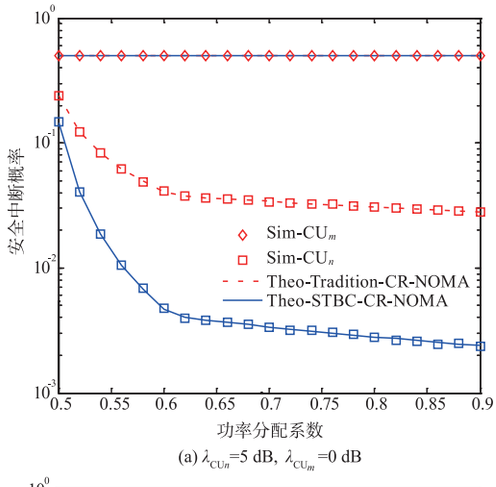


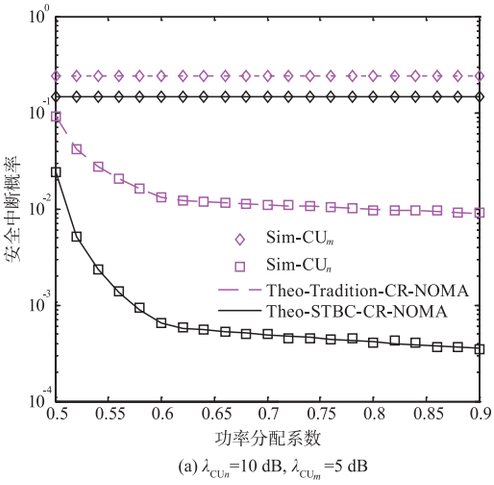
图2　安全中断概率随基站发射功率的变化情况

图 3 为认知用户 CU_n 和 CU_m 的安全中断概率随 CU_m 的功率分配系数 a_m 的变化情况. 从图中可以看出,在 $\lambda_{\mathrm{CU}_n}=5\mathrm{dB}$,$\lambda_{\mathrm{CU}_m}=0\mathrm{dB}$ 和 $\lambda_{\mathrm{CU}_n}=10\mathrm{dB}$,$\lambda_{\mathrm{CU}_m}=5\mathrm{dB}$ 两种情况下,CU_n 的安全中断概率随 CU_m 功率分配系数 a_m 的增大而减小,且在 CR-NOMA 系统中采用 STBC 可降低 CU_n 和 CU_m 的安全中断概率,即提高了系统的安全可靠性,尤其是大幅度降低了信道条件较好用户 CU_n 的安全中断概率;通过提高 BS→CU_i,$i\in\{1,2\}$ 链路的信道条件,也可降低系统的安全中断概率,这

是由于提高 BS→CU_i，$i\in\{1,2\}$链路的信道条件，增加了主信道的信道容量，而窃听信道的信道容量没有发生改变，因此安全中断概率减小，提升了用户的安全可靠性.



(a) λ_{CU_n}=5 dB, λ_{CU_m}=0 dB



(a) λ_{CU_n}=10 dB, λ_{CU_m}=5 dB

图3 安全中断概率随CU_m的功率分配系数a_m的变化情况

图4为认知用户CU_n和CU_m的安全中断概率随主窃听链路信道条件比$\sigma_{me}=\lambda_m/\lambda_e$的变化情况. 其中$\lambda_{CU_n}=\lambda_{CU_m}=\lambda_m=5$dB、$a_m=0.8$、$P_S=10$dB从图中可以看出，$CU_n$和$CU_m$的安全中断概率均随MER的增大而减小，因为MER增加，主信道的信道容量增加，即安全中断概率减小；且从图中可以看出，基于STBC的认知NOMA系统，增加MER，CU_n和CU_m的下降速率更快，这一点对信道条件相对较差的CU_m来说更明显. 且在MER等于10dB时，STBC-CR-NOMA系统中的弱用户CU_m的安全中断概率小于了传统CR-NOMA系统中强用户CU_n的安全中断概率，说明引入STBC可有效提高系统的安全可靠性；从图中还可看出，随着主窃听链路信道条件比的增大，远端用户和近端用户的安全中断性能差值越小.

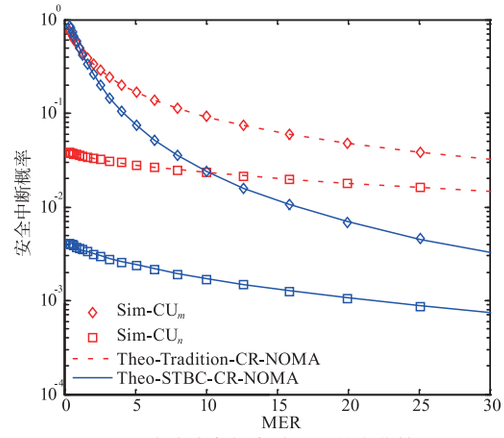
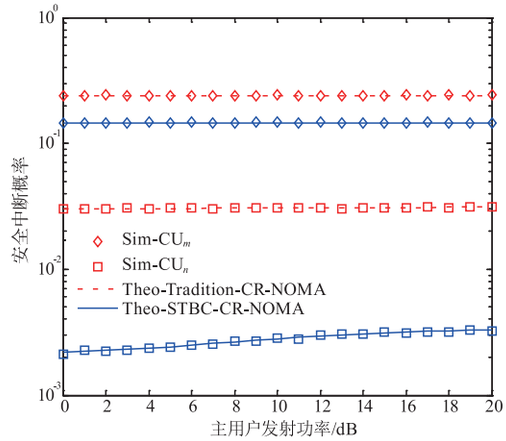
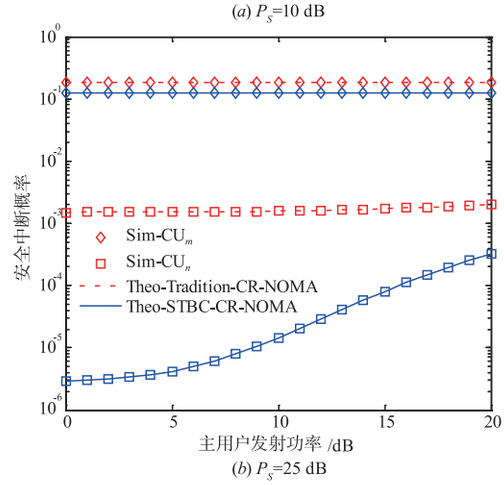


图4 安全中断概率随MER的变化情况

图5为认知用户CU_n和CU_m的安全中断概率随主用户发射功率的变化情况. 其中$\lambda_{CU_n}=\lambda_{CU_m}=\lambda_m=5$dB. 从图中可以看出，不论认知基站发射功率有多高，CU_m的安全中断概率不随主用户发射功率的变化而变化，传统CR-NOMA系统中CU_n的安全中断概率也几乎不随主用户发射功率的变化而变化，而STBC-CR-NOMA



(*a*) P_S=10 dB



(*b*) P_S=25 dB

图5 安全中断概率随主用户发射功率的变化情况

系统中 CU_n 的安全中断概率会随主用户发射功率的变化而变化,当认知基站发射功率较低时即 $P_S = 10$dB,CU_n 的安全中断概率随主用户发射功率变化较小,但当认知基站发射功率较高时即 $P_S = 25$dB,CU_n 的安全中断概率随主用户发射功率变化明显. 因此,通过降低主网络传输干扰,可以降低 STBC-CR-NOMA 系统的 CU_n 用户的安全中断概率,从而提高其安全可靠传输性能.

5　结论

本文将 STBC 应用于无线认知 NOMA 系统中,对基于 STBC 的认知 NOMA 系统中远端认知用户和近端认知用户的物理层安全性能进行了分析,并与传统的无线认知 NOMA 系统中不同用户的物理层安全性能进行比较,发现采用 STBC 可以很大程度上降低认知用户的安全中断概率,尤其是近端用户的安全中断概率. 结果表明,通过调整功率分配系数对远端用户和近端用户的安全传输性能影响不同,而且主用户的干扰对认知系统物理层安全性能影响也不同. 下一步将同时考虑主用户和认知用户的物理层安全性能,设计优化的功率分配方案以提升 underlay 模式下全网用户的安全可靠性传输.

参考文献

[1] Ding Z G, Liu Y W, Choi J H, et al. Application of non-orthogonal multiple access in LTE and 5G networks[J]. IEEE Communications Magazine, 2017, 55(2): 185 – 191.

[2] Yue X W, Qin Z J, Liu Y W, et al. A unified framework for non-orthogonal multiple access[J]. IEEE Transactions on Communications, 2018, 66(11): 5346 – 5359.

[3] Yue X W, Liu Y W, Kang S L, et al. Modeling and analysis of two-way relay non-orthogonal multiple access systems [J]. IEEE Transactions on Communications, 2018, 66(09): 3784 – 3796.

[4] Toka M, Kucur O. Non-orthogonal multiple access with alamouti space-time block coding[J]. IEEE Communications Letters, 2018, 22(09): 1954 – 1957.

[5] Kader M, Shin S Y. Cooperativerelaying using space-time block coded non-orthogonal multiple access[J]. IEEE Transactions on Vehicular Technology, 2017, 66(07): 5894 – 5903.

[6] Liu Y, Ding Z, Elkashlan M, et al. Non-orthogonal multiple access in large-scale underlay cognitive radio networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(12): 10152 – 10157.

[7] Lv L, Chen J, Ni Q. Cooperative non-orthogonal multiple access in cognitive radio[J]. IEEE Communications Letters, 2016, 20(10): 2059 – 2062.

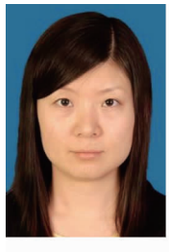
[8] Feng Y, Yan S, Yang Z, et al. Beamforming design and power allocation for secure transmission with NOMA[J]. IEEE Transactions on Communications, 2019, 18(05): 2639 – 2651.

[9] F H Zhou, Z Chu and H J Sun et al. Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 918 – 931.

[10] Zou Y, Wang G. Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack[J]. IEEE Transactions on Industrial Informatics, 2015, 12(2): 780 – 787.

[11] Lei H, Zhang J, Park K H, et al. On secure NOMA systems with transmit antenna selection schemes[J]. IEEE Access, 2017, 5: 17450 – 17464.

作者简介



李美玲　女,1982 年生于山西宁武. 2012 年毕业于北京邮电大学,获博士学位. 现为太原科技大学副教授. 主要研究方向为无线通信关键技术、认知无线网络、协作通信、物理层安全技术、NOMA.

E-mail:meiling_li@126.com

田莉莉(通信作者)　女,1992 年生于山西朔州,现为太原科技大学电子信息工程学院硕士研究生,主要研究方向为无线通信关键技术、非正交多址技术.

E-mail:lili_tian123@163.com

杨晓霞　女,1995 年生于山西阳曲,现为太原科技大学电子信息工程学院硕士研究生,主要研究方向为无线网络的物通信物理层安全性能.

E-mail:2509085887@qq.com

李　莹　女,1994 年生于山西河津,现为太原科技大学电子信息工程学院硕士研究生,主要研究方向为无线认知网络的物理层安全性能.

E-mail:564932926@qq.com